IN THE UNITED STATES
PATENT AND TRADEMARK OFFICE

PATENT APPLICATION

Appellant:	**Danny Raz**	Case:	**RAZ 5 (LCNT/123056)**
Serial No.:	**09/672,206**	Filed:	**9/28/00**
Examiner:	**Paul H. Kang**	Group Art Unit:	**2144**
Title:	**PROCESS TO THWART DENIAL OF SERVICE ATTACKS ON THE INTERNET**		

Confirmation No.:   **8786**

MAIL STOP APPEAL BRIEF-PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

SIR:

APPEAL BRIEF

Appellant submits this Appeal Brief to the Board of Patent Appeals and Interferences on appeal from the decision of the Examiner of Group Art Unit 2616 dated July 25, 2006 finally rejecting claims 1-9.

In the event that an extension of time is required for this appeal brief to be considered timely, and a petition therefor does not otherwise accompany this appeal brief, any necessary extension of time is hereby petitioned for.

The Commissioner is authorized to charge the Appeal Brief fee ($500) and any other fees due to make this filing timely and complete (including extension of time fees) to Deposit Account No. 20-0782/LCNT/123056.

Table of Contents

Real Party in Interest

The real party in interest is LUCENT TECHNOLOGIES INC.

Related Appeals and Interferences

Appellant asserts that no appeals or interferences are known to Appellant, Appellant's legal representative, or assignee which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

Status of Claims

Claims 1-9 are pending in the application. Claims 1-9 were originally presented in the application. Claims 1-9 stand finally rejected as discussed below. The final rejection of claims 1-9 is appealed.

Status of Amendments

All claim amendments have been entered. It should be noted that although the Advisory Action dated October 6, 2006 states that proposed amendments will be entered for purposes of appeal, no amendments were proposed by the Appellant in the response dated September 1, 2006 that was filed in response to the Final Office Action dated July 25, 2006. Appellant respectfully submits that it appears that the Examiner inadvertently checked Box 7 under the AMENDMENTS section of the Advisory Action dated October 6, 2006.

Summary of Claimed Subject Matter

The embodiments of the present invention are generally directed to providing security from attacks made on the legitimate operation of computer networks such as the Internet. More specifically, the embodiments of the present invention are directed to reducing the problems that occur when an attempt is made to interfere with the operation of a network using a coordinated denial of service (DoS) attack. The present invention provides different methods for thwarting coordinated SYN denial of service (CSDoS) attacks against a server disposed in a network of interconnected elements communicating using the TCP protocol. The different embodiments of the present invention use web guard processors, TCP proxies, or processors for thwarting coordinated SYN denial of service (CSDoS) attacks, described herein in additional detail with respect to specific embodiments of the present invention.

A method according to at least one embodiment of the invention includes a method for thwarting coordinated SYN denial of service (CSDoS) attacks against a server disposed in a network of interconnected elements communicating using the TCP protocol. In one embodiment, the method includes controlling a network switch to divert a predetermined fraction of SYN packets destined for the server to a web guard processor, establishing a first TCP connection between one or more clients originating the packets and the web guard processor, and a second TCP connection between the web guard processor and the server, so that packets can be transmitted between the one or more clients and the server, monitoring the number of timed-out connections between the web guard processor and the one or more clients, and, if the number of timed-out connections between the web guard processor and the one or more clients exceeds a first predetermined threshold, controlling the switch to divert all SYN packets destined to the server to the web guard processor.

A method according to at least one embodiment of the invention includes a method for thwarting coordinated SYN denial of service (CSDoS) attacks against a server disposed in a network of interconnected elements communicating using the TCP protocol, where the attack originates from a host generating SYN packets destined for the server. In one embodiment, the method includes arranging a switch receiving the SYN packets destined to the server to forward the SYN packets to a TCP proxy arranged to

operate without an associated cache, sending (for each SYN packet) a SYN/ACK packet from the TCP proxy to a sender address included in the SYN packet by the host, and establishing a TCP connection (corresponding to a particular SYN packet of the SYN packets) between the TCP proxy and the server only if the TCP proxy receives a response from the host to the SYN/ACK packet corresponding to the particular SYN packet.

A method according to at least one embodiment of the invention includes a method for thwarting coordinated SYN denial of service (CSDoS) attacks against a server disposed in a network of interconnected elements communicating using the TCP protocol. In one embodiment, the method includes forwarding a statistical sampling of packets from a switch in the network to a processor and, if packets in the sampling indicate an attack against the server, altering the operation of the switch to forward all packets destined for the server to the processor.

For the convenience of the Board of Patent Appeals and Interferences, Appellant's independent claims 1, 7 and 8 are presented below in claim format with elements read on the various figures of the drawings and appropriate citations to at least one portion of the specification for each element of the appealed claims.

Claim 1 positively recites (with reference numerals, where applicable, and cites to at least one portion of the specification added):

    1. (Previously Presented) A method for thwarting coordinated SYN denial of service (CSDoS) attacks against a server S (120) disposed in a network of interconnected elements (200) communicating using the TCP protocol, comprising the steps of

        controlling a network switch (130-132) to divert a predetermined fraction of SYN packets destined for said server (120), to a web guard processor (201), (Pg. 5, Line 29 – Pg. 6, Line 1)

        establishing a first TCP connection between one or more clients (101-104) originating said packets and said web guard processor (201), and a second TCP connection between said web guard processor (201) and said server (120), so that packets can be transmitted between said one or more clients (101-104) and said server (120), (Pg. 6, Lines 2 – 7)

> monitoring the number of timed-out connections between said web guard processor (201) and said one or more clients (101-104), (Pg. 6, Lines 8-9)
>
> if the number of timed-out connections between said web guard processor (201) and said one or more clients (101-104) exceeds a first predetermined threshold, controlling said switch (130-132) to divert all SYN packets destined to said server (120) to said web guard processor (201). (Pg. 6, Lines 9-13)

Claim 7 positively recites (with reference numerals, where applicable, and cites to at least one portion of the specification added):

> 7. (Previously Presented) A method for thwarting coordinated SYN denial of service (CSDoS) attacks against a server (120) disposed in a network of interconnected elements (200) communicating using the TCP protocol, the attack originating from a host (101-104) generating SYN packets destined for the server (120), said method comprising:
>
> arranging a switch (130-132) receiving the SYN packets destined to the server (120) to forward the SYN packets to a TCP proxy (201) arranged to operate without an associated cache, (Pg. 7, Lines 17-21)
>
> for each SYN packet, sending a SYN/ACK packet from the TCP proxy (201) to a sender address included in the SYN packet by the host (101-104); (Pg. 7, Lines 21-22)
>
> establishing a TCP connection, corresponding to a particular SYN packet of the SYN packets, between the TCP proxy (201) and the server (120) only if the TCP proxy (201) receives a response from the host (101-104) to the SYN/ACK packet corresponding to the particular SYN packet. (Pg. 7, Lines 22-29)

Claim 8 positively recites (with reference numerals, where applicable, and cites to at least one portion of the specification added):

> 8. (Previously Presented) A method for thwarting coordinated SYN denial of service (CSD0S) attacks against a server (120) disposed in a network of interconnected elements (200) communicating using the TCP protocol, comprising:

forwarding a statistical sampling of packets from a switch (130-132) in the network (200) to a processor (201), (Pg. 5, Line 29 – Pg. 6, Line 3)

if packets in the sampling indicate an attack against the server (120), altering the operation of the switch (130-132) to forward all packets destined for the server (120) to the processor (201).

For the convenience of the Board of Patent Appeals and Interferences, Appellant's dependent claim 3 is presented below in claim format with elements read on the various figures of the drawings and appropriate citations to at least one portion of the specification for each element of the appealed claims.

3. (Previously Presented)   The method of claim 1 including the further steps of determining if the number of timed-out connections between said web guard processor (201) and said clients (101-104) exceeds a second predetermined threshold, (Pg. 6, Lines 21-24) and

if so, controlling said switch to delete all SYN packets destined for said server (120). (Pg. 6, Lines 24-26)

Grounds of Rejection to be Reviewed on Appeal

Claims 1-6 and 8-9 are rejected under 35 U.S. C. §103(a) as being unpatentable over U.S. Patent Application Publication Number 2002/0031134 to Poletto et al. (hereinafter Poletto) in view of U.S. Patent Application Publication No. 2002/0035698 to Malan et al. (hereinafter Malan).

Claim 7 is rejected under 35 U.S. C. §103(a) as being unpatentable over Poletto.

Arguments

Rejection Under 35 U.S.C. §103(a)

A.   Claims 1-6 and 8-9:

Claims 1-2 and 4-6:

Claims 1-2 and 4-6 are rejected under 35 U.S. C. §103(a) as being unpatentable over Poletto in view of Malan. Appellant respectfully traverses the rejection.

In general, Poletto discloses a system architecture for thwarting denial of service (DoS) attacks on a victim data center. The system disclosed in Poletto includes monitors deployed in a network. The monitors monitor network traffic flow through the network. The system disclosed in Poletto further includes a central controller that receives data from the monitors. The central controller analyzes network traffic statistics to identify malicious network traffic. (Poletto, Abstract).

Poletto, however, fails to teach or suggest Appellant's claim 1, as a whole. Namely, as admitted by the Examiner, Poletto fails to teach or suggest at least the limitations of "controlling a network switch to divert a predetermined fraction of SYN packets destined for said server, to a web guard processor" and "monitoring the number of timed-out connections between said web guard processor and said one or more clients, and, if the number of timed-out connections between said web guard processor and said one or more clients exceeds a first predetermined threshold, controlling said switch to divert all SYN packets destined to said server to said web guard processor," as claimed in Appellant's claim 1.

As such, in at least the Final Office Action dated July 25, 2006, the Examiner cites Malan, asserting that Malan teaches limitations of Appellant's claim 1 which are not taught by Poletto. Malan, however, fails to bridge the substantial gap as between Poletto and Appellant's invention.

In general, Malan discloses a system for protecting publicly accessible network computer services from undesirable network traffic. Network traffic destined for the

network computer services is received and analyzed in order to identify an undesirable user of the services. As disclosed in Malan, topologically anomalous application-level patterns of traffic are identified and removed from the network. (Malan Abstract). As further disclosed in Malan, network topology information and coarse-grained traffic statistics from routers are used to detect, backtrack, and filter network attacks.

Malan, however, is devoid of any teaching or suggestion of diverting a predetermined fraction of SYN packets destined for a server to a processor. Furthermore, Malan is devoid of any teaching or suggestion of monitoring the number of timed-out connections between said web guard processor and said one or more clients, and, if the number of timed-out connections between said web guard processor and said one or more clients exceeds a first predetermined threshold, controlling said switch to divert all SYN packets destined to said server to said web guard processor, as claimed in Appellant's claim 1.

More specifically, in the Final Office Action dated July 25, 2006, the Examiner cites a specific portion of Malan for teaching Appellant's limitations of "controlling a network switch to divert a predetermined fraction of SYN packets destined for said server, to a web guard processor" and "monitoring the number of timed-out connections between said web guard processor and said one or more clients, and, if the number of timed-out connections between said web guard processor and said one or more clients exceeds a first predetermined threshold, controlling said switch to divert all SYN packets destined to said server to said web guard processor," as claimed in Appellant's claim 1. The cited portions of Malan, however, merely state the following:

> "[0108] FIG. 10 demonstrates the utility of the StormDetector system. A host in ISP-A is bombarding a target server in the Web hosting service with a denial of service attack. However, the attacker is forging the return address on the packets in the attack, making is impossible to determine their true origin. The StormDetector's analysis engine receives flow statistics from the routers in the target's hosting service. From these statistics, it can detect the attack at some-set of the affected routers along its path. This path leads directly from the target to ISP-A's border, where the attack originates. This example demonstrates the utility of the StormDetector deployed within a Web hosting service's network. It can also be used in both source and transit networks.

[0109] When employed at an attacker's originating network, StormDetector can pinpoint the location of the attacker. In this case, it will backtrack the attack directly to its source's first-hop router. It may be that the attacker is a zombie residing on a compromised machine in an enterprise network. In addition to uncovering those traditional launchpads, StormDetector will be instrumental in identifying attacks originating from home machines that connect to the Internet through persistent tier-2 ISP's ADSL or cable modem connections.

[0110] FIG. 9 represents the process for detecting anomalies in the network statistics within a single zone. At the start, the system picks a measurement node at random. A set of coarse flow statistics or packet header samples is collected. This set of statistics is examined for anomalies. These anomalies include both clearly defined misuse of the network resources, and also significant differences between the profile of the various endpoints and the behavior measured in the sample. If any new anomalies are detected in the sample, they are added as conditional anomalies, and the collector is updated with these new conditional anomalies. Next, a refined sample is taken with respect to the pending conditional anomalies at the collector. The system then looks at the refined sample of the network statistics for the presence of both new conditional anomalies as well as old anomalies. For each anomaly found, its status is updated. The system then goes through the outstanding anomalies and prunes out any stale ones. Finally, the system updates the database with the latest summary statistics for each of the outstanding anomalies. The system then repeats, by beginning at the start node."
[Malan, Para. 0108 – 0110].

The cited portion of Malan is entirely different than Appellant's claim 1. The cited portion of Malan merely describes a StormDetector system that receives flow statistics from routers in the target's hosting service, and from those received flow statistics, detects the attack at some set of the affected routers along a path from the target of the attack to the border of the ISP where the attack originates. The StormDetector system pinpoints the location of the attacker by backtracking the attack directly to its source's first-hop router. Furthermore, the cited portion of Malan further describes a process for analyzing collected statistics in order to detect anomalies in the collected statistics.

In other words, the cited portion of Malan is completely devoid of any teaching or suggestion of diverting any traffic from a server to a processor. Rather, Milan merely teaches collecting flow <u>statistics</u> at routers and forwarding the flow <u>statistics</u> from the

514037-1

routers to the StormDetector's analysis engine for use in backtracking the source of the attack. Malan doesn't teach or suggest diverting the actual <u>traffic</u> from the routers to the StormDetector's analysis engine, or any other processor for that matter. The sending of <u>flow statistics</u>, as taught in Malan, is not diverting a predetermined fraction of SYN <u>packets</u> destined for said server, to a web guard processor, as claimed in Appellant's claim 1. As such, Malan fails to teach or suggest "controlling a network switch to divert a predetermined fraction of SYN packets destined for said server, to a web guard processor," as claimed in Appellant's claim 1.

Furthermore, the cited portion of Malan is completely devoid of any teaching or suggestion of any connections between clients and a processor or between the processor and a server, much less timed-out connections, monitoring the number of timed-out connections, or taking any action in response to the number of timed-out connections exceeding a threshold. Rather, Malan teaches analysis of network topology information and flow statistics to detect an attack at some-set of the affected routers along a path, and tracing the path from the target to the border router where the attack originates. As such, Malan also fails to teach or suggest the limitations of "monitoring the number of timed-out connections between said web guard processor and said one or more clients" and "if the number of timed-out connections between said web guard processor and said one or more clients exceeds a first predetermined threshold, controlling said switch to divert all SYN packets destined to said server to said web guard processor," as claimed in Appellant's claim 1.

Moreover, even if Malan did teach monitoring for such timed-out connections and taking action in response to the number of timed-out connections between clients and the processor (which Appellant respectfully submits that Malan does not), Malan would still fail to teach or even suggest diverting all SYN packets destined to the server to the web guard processor, as claimed in Appellant's claim 1. Rather, Malan merely teaches that once the attack has been traced to the source of the attack, a filtering rule is applied to the attacker's router to remove its traffic from the network. (Malan, Para. 0115). Specifically, Malan states that "[o]nce these malicious hosts are identified, their requests can be filtered either at the server or upstream in the network." (Malan, Para. 0060). The <u>filtering</u> of requests, as taught in Malan, does not teach or suggest <u>diverting all SYN</u>

packets destined to the server to the web guard processor, as claimed in Appellant's claim 1. As such, Malan fails to teach or suggest the limitation of "controlling said switch to divert all SYN packets destined to said server to said web guard processor," as claimed in Appellant's claim 1.

As such, Poletto and Malan, alone or in combination, fail to teach or suggest Appellant's claim 1, as a whole.

The test under 35 U.S.C. §103 is not whether an improvement or a use set forth in a patent would have been obvious or non-obvious; rather the test is whether the claimed invention, considered as a whole, would have been obvious. Jones v. Hardy, 110 USPQ 1021, 1024 (Fed. Cir. 1984) (emphasis added). Moreover, the invention as a whole is not restricted to the specific subject matter claimed, but also embraces its properties and the problem it solves. In re Wright, 6 USPQ 2d 1959, 1961 (Fed. Cir. 1988) (emphasis added). Poletto and Malan, alone or in combination, fail to teach or suggest Appellant's claim 1, as a whole.

As such, Appellant submits that independent claim 1 is not obvious and fully satisfies the requirements of 35 U.S.C. §103 and is patentable thereunder. Furthermore, claims 2 and 4-6 depend, either directly or indirectly, from independent claim 1 and recite additional limitations therefor. As such, for at least the same reasons discussed above, these dependent claims also are not obvious and fully satisfy the requirements of 35 U.S.C. §103 and are patentable thereunder.

Accordingly, Appellant respectfully requests that the rejection of the claims be withdrawn.

Claim 3:

Claim 3 is rejected under 35 U.S. C. §103(a) as being unpatentable over Poletto in view of Malan. Appellant respectfully traverses the rejection.

As described hereinabove, Poletto and Malan, alone or in combination, fail to teach or suggest Appellant's claim 1, as a whole. Namely, Poletto and Malan fail to teach or suggest at least the limitations of "controlling a network switch to divert a predetermined fraction of SYN packets destined for said server, to a web guard processor" and "monitoring the number of timed-out connections between said web

guard processor and said one or more clients, and, if the number of timed-out connections between said web guard processor and said one or more clients exceeds a first predetermined threshold, controlling said switch to divert all SYN packets destined to said server to said web guard processor," as claimed in Appellant's claim 1.

Furthermore, claim 3 depends from claim 1, and recites additional limitations therefor. As such, for at least the reasons described hereinabove with respect to claim 1, Appellant submits that Poletto and Malan also fail to teach or suggest Appellant's claim 3, as a whole. Furthermore, Poletto and Malan, alone or in combination, fail to teach or suggest at least the additional limitations of Appellant's claim 3. Namely, Poletto and Malan, alone or in combination, also fail to teach or suggest the limitation of "determining if the number of timed-out connections between said web guard processor and said clients exceeds a second predetermined threshold," as claimed in Appellant's claim 3.

As described herein, as admitted by the Examiner, Poletto fails to teach or suggest the limitation of "monitoring the number of timed-out connections between said web guard processor and said one or more clients, and, if the number of timed-out connections between said web guard processor and said one or more clients exceeds a first predetermined threshold," performing an action, as claimed in Appellant's claim 1. Similarly, since Poletto fails to teach or suggest the limitation associated with the first predetermined threshold of Appellant's claim 1, Poletto also fails to teach or suggest the similar limitation of "determining if the number of timed-out connections between said web guard processor and said clients exceeds a second predetermined threshold," as claimed in Appellant's claim 3.

Furthermore, Malan fails to bridge the substantial gap as between Poletto and Appellant's claim 3. As described herein, Malan is completely devoid of any teaching or suggestion of any connections between clients and a processor or between the processor and a server, much less timed-out connections, monitoring the number of timed-out connections, or taking any action in response to the number of timed-out connections exceeding a threshold. Rather, Malan teaches analysis of network topology information and flow statistics to detect an attack at some-set of the affected routers along a path, and tracing the path from the target to the border router, where the attack originates. As such,

Malan fails to teach or suggest the limitation of "determining if the number of timed-out connections between said web guard processor and said clients exceeds a second predetermined threshold," as claimed in Appellant's claim 3.

As such, Poletto and Malan, alone or in combination, fail to teach or suggest Appellant's claim 3, as a whole.

The test under 35 U.S.C. §103 is not whether an improvement or a use set forth in a patent would have been obvious or non-obvious; rather the test is whether the claimed invention, considered as a whole, would have been obvious. Jones v. Hardy, 110 USPQ 1021, 1024 (Fed. Cir. 1984) (emphasis added). Moreover, the invention as a whole is not restricted to the specific subject matter claimed, but also embraces its properties and the problem it solves. In re Wright, 6 USPQ 2d 1959, 1961 (Fed. Cir. 1988) (emphasis added). Poletto and Malan, alone or in combination, fail to teach or suggest Appellant's claim 3, as a whole.

As such, Appellant submits that claim 3 is not obvious and fully satisfies the requirements of 35 U.S.C. §103 and is patentable thereunder.

Accordingly, Appellant respectfully requests that the rejection of the claims be withdrawn.

Claims 8-9:

Claims 8-9 are rejected under 35 U.S. C. §103(a) as being unpatentable over Poletto in view of Malan. Appellant respectfully traverses the rejection.

As described hereinabove with respect to claim 1, Poletto discloses a system architecture for thwarting denial of service (DoS) attacks on a victim data center. The system disclosed in Poletto includes monitors that monitor network traffic flow through the network, and a central controller that receives network traffic statistics from the monitors. The central controller analyzes the network traffic statistics to identify malicious network traffic. (Poletto, Abstract).

Poletto, however, fails to teach or suggest Appellant's claim 8, as a whole. Namely, Poletto fails to teach or suggest the limitations of "forwarding a statistical sampling of packets from a switch in the network to a processor" and "if packets in the sampling indicate an attack against the server, altering the operation of the switch to

forward all packets destined for the server to the processor," as claimed in Appellant's claim 8.

Rather, Poletto merely discloses that a plurality of traffic monitors monitor traffic flow through the network, and collect network traffic statistics. The network traffic statistics are sent to a central controller for processing. Specifically, as taught in Poletto, the central controller analyzes network traffic statistics to identify malicious network traffic. In other words, the system of Poletto sends <u>statistics</u> associated with packets to the central controller, <u>not the actual packets themselves</u>. Thus, the collection of network traffic <u>statistics</u> and sending of the network traffic <u>statistics</u> to a central controller for analysis, as taught in Poletto, is not forwarding a statistical sampling of <u>packets</u> from a switch in the network to a processor, as claimed in Appellant's claim 8.

Furthermore, Poletto also discloses a gateway supporting a monitoring process that examines a ratio of incoming TCP packets to outgoing TCP packets for a particular set of machines, such as web servers. The monitoring process compares the ratio to a threshold. The monitoring process stores the ratio and conducts an ongoing analysis to determine how the ratio changes over time. Specifically, as taught in Poletto, as the ratio grows increasingly beyond 2:1, it is an increasing indication that the machines are receiving bad TCP traffic. The ratio is measured using a multiple-bucket algorithm in which the gateway divides traffic into multiple buckets by source network address, and tracks the ratio of incoming to outgoing traffic for each bucket. (Poletto, Para. 0053-0054).

In other words, the gateway of Poletto merely teaches categorization of received packets into different buckets, and monitoring, for each of the buckets, a ratio of incoming TCP packets to outgoing TCP packets. The gateway disclosed in Poletto does not forward packets to any processor, much less forward a statistical sampling of the packets to a processor, as claimed in Appellant's claim 8. Rather, as described herein, the gateway of Poletto merely categorizes received packets locally at the gateway and monitors a ratio associated with each bucket into which the packets are categorized.

Furthermore, even assuming that Poletto forwards the ratio information from the gateway to a central controller, Poletto would still only teach sending statistics associated with packets to the central controller, not the actual packets themselves. As described

above, sending of the network traffic statistics to a central controller, as taught in Poletto, is not forwarding a statistical sampling of packets from a switch in the network to a processor. As such, Poletto would still fail to teach or suggest forwarding a statistical sampling of packets from a switch in the network to a processor, as claimed in Appellant's claim 8.

In the Final Office Action dated July 25, 2006, the Examiner asserts that Poletto teaches forwarding a statistical sampling of packets from a switch in a network to a processor. (Final Office Action, Pg. 3). Appellant respectfully disagrees. From the teachings of Poletto described hereinabove, it is clear that, at most, Poletto teaches collection of network traffic statistics and sending of the network traffic statistics to a central controller for analysis. In Poletto, however, the actual packets from which the statistics are collected are not forwarded from a network switch to a processor. Rather, Poletto only discloses forwarding of statistics associated with packets. As such, Poletto fails to teach or suggest forwarding a statistical sampling of packets from a switch in the network to a processor, as claimed in Appellant's claim 8.

Furthermore, since, as described hereinabove, Poletto fails to teach or suggest even sending a statistical sampling of packets from a switch to a processor, Poletto must also fails to teach or suggest altering the operation of a switch to forward all packets destined for the server to the processor, as claimed in Appellant's claim 8.

As such, Poletto fails to teach or suggest Appellant's claim 8, as a whole. Furthermore, Malan fails to bridge the substantial gap as between Poletto and Appellant's claim 8. Namely, Malan fails to teach or suggest the limitations of "forwarding a statistical sampling of packets from a switch in the network to a processor" and "if packets in the sampling indicate an attack against the server, altering the operation of the switch to forward all packets destined for the server to the processor," as claimed in Appellant's claim 8.

In the Final Office Action dated July 25, 2006, the Examiner cites a specific portion of Malan for teaching the limitations of Appellant's claim 8. Specifically, the Examiner cites paragraphs 0108 – 0110 for teaching the limitations of Appellant's claim 8.

As described hereinabove with respect to claim 1, however, the cited portion of Malan merely teaches a StormDetector system that receives flow statistics from routers in the target's hosting service, and from those received statistics, detects the attack at some set of the affected routers along a path from the target of the attack to the border of the ISP where the attack originates. The StormDetector system pinpoints the location of the attacker by backtracking the attack directly to its source's first-hop router. The cited portion of Malan further describes a process for analyzing collected statistics in order to detect anomalies in the collected statistics.

In other words, Malan is devoid of any teaching or suggestion of forwarding any packets from a network switch to a processor, much less forwarding a statistical sampling of packets from a network switch to a processor, as claimed in Appellant's claim 8. Rather, Milan merely teaches collecting flow <u>statistics</u> at routers and forwarding the flow <u>statistics</u> from the routers to the StormDetector's analysis engine for use in backtracking the source of the attack. Malan doesn't teach or suggest diverting the actual <u>packets</u> from which the statistics are determined from the routers to the StormDetector's analysis engine, much less forwarding a statistical sampling of packets. The sending of flow statistics, as taught in Malan, is not forwarding of packets, as claimed in Appellant's claim 8. As such, Malan fails to teach or suggest "forwarding a statistical sampling of packets from a switch in the network to a processor," as claimed in Appellant's claim 8.

Furthermore, Malan also fails to teach or suggest the limitation of "if packets in the sampling indicate an attack against the server, altering the operation of the switch to forward all packets destined for the server to the processor," as claimed in Appellant's claim 8.

As such, Poletto and Malan, alone or in combination, fail to teach or suggest Appellant's claim 8, as a whole.

The test under 35 U.S.C. §103 is not whether an improvement or a use set forth in a patent would have been obvious or non-obvious; rather the test is whether the claimed invention, <u>considered as a whole</u>, would have been obvious. <u>Jones v. Hardy</u>, 110 USPQ 1021, 1024 (Fed. Cir. 1984) (emphasis added). Moreover, the invention <u>as a whole</u> is not restricted to the specific subject matter claimed, but also embraces its properties and the problem it solves. <u>In re Wright</u>, 6 USPQ 2d 1959, 1961 (Fed. Cir. 1988) (emphasis

added). Poletto and Malan, alone or in combination, fail to teach or suggest Appellant's claim 8, as a whole.

As such, Appellant submits that independent claim 8 is not obvious and fully satisfies the requirements of 35 U.S.C. §103 and is patentable thereunder. Furthermore, claim 9 depends from independent claim 8 and recites additional limitations therefor. As such, for at least the same reasons discussed above, claim 9 is also not obvious and fully satisfy the requirements of 35 U.S.C. §103 and is patentable thereunder.

Accordingly, Appellant respectfully requests that the rejection of the claims be withdrawn.

B.   Claim 7:

Claim 7 is rejected under 35 U.S. C. §103(a) as being unpatentable over Poletto. In the Final Office Action dated July 25, 2006, however, the Examiner merely cites Poletto against Appellant's claim 7. (Final Office Action, Pg. 3). The Examiner does not reference Malan in the rejection of claim 7. Furthermore, the Examiner does not describe any modification to Poletto to arrive at Appellant's claim 7, nor does the Examiner cite general knowledge of one skilled in the art. Appellant respectfully traverses the rejection.

As described herein, Poletto discloses a system architecture for thwarting denial of service attacks on a victim data center. The system includes monitors that monitor network traffic flow through the network, and a central controller that receives data from the plurality of monitors. The central controller analyzes network traffic statistics to identify malicious network traffic. (Poletto, Abstract). Poletto, however, fails to teach or suggest any of the elements of Appellant's claim 7. Specifically, Appellant's claim 7 recites:

> "A method for thwarting coordinated SYN denial of service
> (CSDoS) attacks against a server disposed in a network of interconnected
> elements communicating using the TCP protocol, the attack originating from a
> host generating SYN packets destined for the server, said method comprising:
>   arranging a switch receiving the SYN packets destined to the server to
> forward the SYN packets to a TCP proxy arranged to operate without an
> associated cache,
>   for each SYN packet, sending a SYN/ACK packet from the TCP proxy to
> a sender address included in the SYN packet by the host;

establishing a TCP connection, corresponding to a particular SYN packet of the SYN packets, between the TCP proxy and the server only if the TCP proxy receives a response from the host to the SYN/ACK packet corresponding to the particular SYN packet."
(Emphasis added).

Appellant's claim 7 discloses that a switch receiving SYN packets from a client intended for a server is arranged to forward the SYN packets to a TCP proxy arranged to operate without an associated cache. For each SYN packet received by the TCP proxy, the TCP proxy sends a SYN/ACK packet to the sender address included in the SYN packet. If the TCP proxy receives a response from the host to the SYN/ACK packet, the TCP proxy establishes a TCP connection between the TCP proxy and the server for which the SYN packet was intended. As such, as taught in Appellant's claim 7, the server is isolated from the TCP handshake process by the TCP proxy. The TCP proxy of Appellant's invention verifies the TCP handshake before the TCP proxy completes the connection between the host and the server by establishing a TCP connection between TCP proxy and server.

By contrast, Poletto teaches a gateway disposed between a client and a server. The gateway receives a SYN packet from the client and forwards the SYN packet to the server. In other words, as taught in Poletto, the gateway forwards the SYN packet to the server for which the packet is intended. The forwarding of a SYN packet from the server for which the packet is intended, as taught in Poletto, is not forwarding SYN packets to a TCP proxy, as claimed in Appellant's claim 7. As such, Poletto does not teach or suggest Appellant's limitation of arranging a switch receiving the SYN packets destined to the server to forward the SYN packets to a TCP proxy arranged to operate without an associated cache, as claimed in Appellant's claim 7.

In further contrast to Appellant's claim 7, Poletto teaches that the server generates the SYN/ACK packet in response to the SYN packet, and sends the SYN/ACK packet to the gateway, which forwards the SYN/ACK packet to the associated client. In other words, as taught in Poletto, the server for which the SYN packet was intended sends the associated SYN/ACK packet to the client. Although the SYN/ACK packet in the Poletto system traverses the gateway in the path between the server the client, the SYN/ACK packet is not sent from the gateway. A SYN/ACK packet sent from a server to a client,

as taught in Poletto, is not a SYN/ACK packet that is sent <u>from a TCP proxy</u> to the <u>sender</u> address included in the SYN packet by the host, as claimed in Appellant's claim 7. As such, Poletto does not teach Appellant's limitation that the SYN/ACK packet is sent <u>from a TCP proxy</u> to the sender address included in the SYN packet by the host, as taught in Appellant's claim 7.

In further contrast to Appellant's claim 7, Poletto teaches that the <u>gateway sends an ACK packet to the server</u> to close the three-way handshake. By contrast, since, as taught in Appellant's claim 7, the <u>TCP proxy sends a SYN/ACK packet back to the host</u> in response to the SYN packet, Appellant's claim 7 teaches that the <u>TCP proxy waits until it receives, from the host, a response to the SYN/ACK packet</u>. The transmission of an ACK packet <u>from a gateway to a server</u> in response to a SYN/ACK packet <u>received by the gateway from the server</u>, as taught in Poletto, is not transmission of a response <u>from the client to the TCP proxy</u> in response to a SYN/ACK packet received by <u>the client from the TCP proxy</u>, as claimed in Appellant's claim 7.

Furthermore, as taught in Appellant's claim 7, if the TCP proxy receives, from the host, a response to the SYN/ACK packet, the TCP proxy completes the connection between the host and the server by <u>establishing a TCP connection between the TCP proxy and the server</u>. There is no teaching or suggestion in Poletto that the gateway establishes a TCP connection to the server. This is simply not required in the Poletto system since there is already a TCP connection between the client and the server which is used in the TCP handshake process. As such, Poletto fails to teach or suggest Appellant's limitation of "establishing a TCP connection, corresponding to a particular SYN packet of the SYN packets, between the TCP proxy and the server only if the TCP proxy receives a response from the host to the SYN/ACK packet corresponding to the particular SYN packet," as claimed in Appellant's claim 7.

Moreover, although the Examiner fails to put forth any argument that Malan discloses that which is missing from Poletto, Appellant respectfully notes that Malan also fails to teach or suggest any of the limitations as claimed in Appellant's claim 7. Rather, as described hereinabove with respect to claim 1, Malan merely teaches a StormDetector system that receives flow statistics from routers in the target's hosting service, and from those received statistics, detects the attack at some set of the affected routers along a path

from the target of the attack to the border of the ISP where the attack originates. The StormDetector system pinpoints the location of the attacker by backtracking the attack directly to its source's first-hop router. The cited portion of Malan further describes a process for analyzing collected statistics in order to detect anomalies in the collected statistics.

Malan, however, fails to teach or suggest arranging a switch receiving SYN packets destined to a server to forward the SYN packets to a TCP proxy, much less a TCP proxy arranged to operate without an associated cache. Furthermore, Malan fails to teach or suggest sending for each SYN packet a SYN/ACK packet from the TCP proxy to a sender address included in the SYN packet by the host. Moreover, Malan fails to teach or suggest establishing a TCP connection, corresponding to a particular SYN packet of the SYN packets, between the TCP proxy and the server only if the TCP proxy receives a response from the host to the SYN/ACK packet corresponding to the particular SYN packet.

As such, Poletto and Malan, alone or in combination, fail to teach or suggest Appellant's claim 7, as a whole.

The test under 35 U.S.C. §103 is not whether an improvement or a use set forth in a patent would have been obvious or non-obvious; rather the test is whether the claimed invention, considered as a whole, would have been obvious. Jones v. Hardy, 110 USPQ 1021, 1024 (Fed. Cir. 1984) (emphasis added). Moreover, the invention as a whole is not restricted to the specific subject matter claimed, but also embraces its properties and the problem it solves. In re Wright, 6 USPQ 2d 1959, 1961 (Fed. Cir. 1988) (emphasis added). Poletto and Malan, alone or in combination, fail to teach or suggest Appellant's claim 7, as a whole.

As such, Appellant submits that independent claim 7 is not obvious and fully satisfies the requirements of 35 U.S.C. §103 and is patentable thereunder.

Moreover, as described hereinabove, in the Final Office Action dated July 25, 2006 the Examiner merely relied on the teachings of Poletto for rejecting Appellant's claim 8. As such, although the Appellant believes that the Examiner should have applied a rejection under 35 U.S.C. §102 rather than 35 U.S.C. §103 (because the Examiner did not modify Poletto or cite knowledge of one skilled in the art in applying the rejection),

the Appellant respectfully submits that since Appellant's claim 7 is patentable over Poletto in view of Malan under 35 U.S.C. §103, Appellant's claim 7 is also patentable over Poletto under 35 U.S.C. §102.

Accordingly, Appellant respectfully requests that the rejection of the claims be withdrawn.
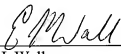
Conclusion

Thus, Appellant submits that none of the claims presently in the application are allowable under the provisions of 35 U.S.C. §103.

For the reasons advanced above, Appellant respectfully urges that the rejections of claims 1-9 are improper. Reversal of the rejections of the Final Office Action is respectfully requested.

Respectfully submitted,

Dated: 12/19/06

Eamon J. Wall
Registration No. 39,414
Patterson & Sheridan, L.L.P.
595 Shrewsbury Ave. Suite 100
Shrewsbury, NJ 07702
Telephone: (732) 530-9404
Facsimile: (732) 530-9808
Attorney for Appellant

CLAIMS APPENDIX

1. (Previously Presented)   A method for thwarting coordinated SYN denial of service (CSDoS) attacks against a server S disposed in a network of interconnected elements communicating using the TCP protocol, comprising the steps of

controlling a network switch to divert a predetermined fraction of SYN packets destined for said server, to a web guard processor,

establishing a first TCP connection between one or more clients originating said packets and said web guard processor, and a second TCP connection between said web guard processor and said server, so that packets can be transmitted between said one or more clients and said server,

monitoring the number of timed-out connections between said web guard processor and said one or more clients,

if the number of timed-out connections between said web guard processor and said one or more clients exceeds a first predetermined threshold, controlling said switch to divert all SYN packets destined to said server to said web guard processor.

2. (Previously Presented)   The method of claim 1 further comprising the step of generating an alarm indicating that said server is likely to be under attack.

3. (Previously Presented)   The method of claim 1 including the further steps of

determining if the number of timed-out connections between said web guard processor and said clients exceeds a second predetermined threshold, and

if so, controlling said switch to delete all SYN packets destined for said server.

4. (Previously Presented)   The method of claim 3 further comprising the step of generating an alarm indicating that said server is under attack.

5. (Original)   The method of claim 1 further including the step of notifying said server that it is under attack.

6. (Original) The method of claim 1 further including the step of notifying other web guard processors in said network that said server is under attack.

7. (Previously Presented) A method for thwarting coordinated SYN denial of service (CSDoS) attacks against a server disposed in a network of interconnected elements communicating using the TCP protocol, the attack originating from a host generating SYN packets destined for the server, said method comprising:

arranging a switch receiving the SYN packets destined to the server to forward the SYN packets to a TCP proxy arranged to operate without an associated cache,

for each SYN packet, sending a SYN/ACK packet from the TCP proxy to a sender address included in the SYN packet by the host;

establishing a TCP connection, corresponding to a particular SYN packet of the SYN packets, between the TCP proxy and the server only if the TCP proxy receives a response from the host to the SYN/ACK packet corresponding to the particular SYN packet.

8. (Previously Presented) A method for thwarting coordinated SYN denial of service (CSD0S) attacks against a server disposed in a network of interconnected elements communicating using the TCP protocol, comprising:

forwarding a statistical sampling of packets from a switch in the network to a processor,

if packets in the sampling indicate an attack against the server, altering the operation of the switch to forward all packets destined for the server to the processor.

9. (Previously Presented) The method of claim 8 wherein the switch is arranged to discard packets in the event an attack is detected.

EVIDENCE APPENDIX

None

RELATED PROCEEDINGS APPENDIX

None